UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------X

UNITED STATES OF AMERICA :

S2 17 Cr. 548 (PAC)

-v- :

JOSHUA ADAM SCHULTE,

Defendant. :

----------X

DECLARATION OF STEVEN M. BELLOVIN, Ph.D.

STEVEN M. BELLOVIN, Ph.D., declares under penalty of perjury:

1. I am the Percy K. and Vida L.W. Hudson Professor of Computer Science and affiliate law faculty at Columbia University. I was retained by defense counsel in this case to assist as an expert in computer systems and computer security. I make this declaration in support of Mr. Schulte's motion for a mistrial and, more specifically, to reply to some of the points made by the government in opposition to that motion. This declaration is based on my personal knowledge and more than 50 years of experience as a computer expert.

2. I have reviewed the government's letter to the Court, dated February 19, 2020, opposing Mr. Schulte's motion for a mistrial ("Gov't Opp."). The government claims, in summary, that the defense has not been prejudiced by the government's decision to grant its forensic expert Patrick Leedom—but

not me or defense counsel—access to the "mirror images" of the CIA's ESXi Server and NetApp Server (also known as the FSO1 Server). The government asserts that "the defense has had all of the information upon which Mr. Leedom relied to arrive at his opinions well before trial, and thus a reasonable opportunity to test and scrutinize those opinions." Gov't Opp. at 14.

3. The government's assertions are not accurate. As discussed below, because I was never granted access to the mirror images, I have been unable to reproduce (and thereby confirm or refute) all the analyses and tests that Mr. Leedom was able to perform. While the government notes that it has made a substantial amount of forensic material available to the defense, this material is far from complete, and is not usable to conduct certain analyses that the government's expert was able to conduct. Those analyses require examination of the mirror images.

4. The government makes a number of specific assertions that are misleading or simply false. For example, the government states that certain FBI reports "make clear that Michael never had Atlassian administrator privileges and thus did not have the ability to access or copy the Altabackups (from which the Vault 7 information was stolen)." Gov't Opp. at 8. As a simple factual matter, this statement is untrue. The possession of "Atlassian administrator privileges" had nothing to do with the ability to access or copy the Altabackup files. Rather, what was needed was *log-in access*, i.e., a working user name

and password, to the Confluence Virtual Machine (or "VM"). Michael certainly had such log-in access. As shown in Leedom Slide 60 (GX 1207-10 and GX 1207-11), which is described as "April 16, 2016 Confluence Backup—password and shadow files," a user name called "confluence" is listed (Slide 60, GX 1207-11, third line from the bottom). The password for this user name was listed on a web page that was accessible to all OSB members, including Michael, and was used for many other log-ins throughout the organization. *See* GX 1202-5 (listing one commonly used password as "123ABCdef."). This password was valid both before and after April 16, 2016. So if Michael had simply typed that password into the Confluence VM on April 20, 2016, along with the user name "confluence," he would have had access to the Altabackup files from which the Vault 7 information was allegedly taken.

5. Any experienced computer programmer would have known that there was very likely to be a user name "confluence" on the Confluence VM. On Linux systems, it is normal to have a separate user name for any software packages that manage their own data; this includes Confluence and all other elements of the Atlassian software suite. There are several other examples of this in just the Confluence password and shadow files. It is customary to use the name of the software package, e.g., "confluence" as the user name. Again, this is evident on the Confluence VM itself.

6. The above point demonstrates, contrary to the government's assertions, that Michael had the ability to access and copy the March 3, 2016 Confluence and

Stash backup files that the government claims were eventually sent to WikiLeaks.

7. The government also asserts that it has provided large amounts of information to the defense, including log files, but this data is in no way equivalent to the information to which Mr. Leedom has had access.

8. The government claims that it gave the defense log files from the ESXi server. In fact—per the defense *ex parte* letter to the Court of February 12, 2019—some of those files were demonstrably damaged. Such damage was likely the result of prior forensic examination, which the government was able to perform on the original image of the server. Had the defense been provided with a full mirror image of the ESXi server, the defense would have been able to conduct its own examination of the files in their original state.

9. The government claims that it provided the Confluence databases to the defense. But those databases appear to have been heavily redacted, with all content files either missing or deleted, including those allegedly released by WikiLeaks. Furthermore, they did not include the apparently damaged "SQL" file that Mr. Berger evidently used in his analyses. GX 1704, Slide 3 (GX 1207-97). If the defense had a full copy of the SQL file—not simply a file embedded as part of a forensic case—the defense could have done other SQL queries to establish whether the data could have been taken from a later backup file.

10. The government claims that defense had the "backup script" in sufficient time to determine whether Mr. Leedom's claims about the damage to the SQL file are accurate. In fact, without access the mirror images, and for reasons too complex and technical to explain here, the backup script alone does not permit the defense to assess the validity of all of Mr. Leedom's assertions.

11. The government claims that it has produced to the defense all of the unallocated space from the ESXi server "about which Mr. Leedom testified." Gov't Opp. at 19 ¶ 6. But "the unallocated space …about which Mr. Leedom *testified*" (emphasis added) is not the same as all the unallocated space he *examined*. If I had been granted access to the examined space, there is a reasonable probability I would have discovered evidence, including potentially exculpatory evidence, that Mr. Leedom either missed or ignored.

I declare under penalty of perjury that the foregoing is true and correct.

/s/

Steven M. Bellovin, Ph.D.

February 22, 2020